Wer überwacht die Überwacher? Kernbereichsschutz beim Bundeskriminalamt durch eine „unabhängige Stelle“

Gastautor 2016-07-07T08:43:43

von JOHANNA DECHER

Im Schatten der Fußballeuropameisterschaft verabschiedete der Bundestag am 24.06.2016 im Eilverfahren ein neues Anti-Terror-Paket. Auch dieses steht in der scharfen Kritik der Opposition und zivilgesellschaftlicher Vereinigungen und wird voraussichtlich den Weg zum BVerfG finden. Für die Beurteilung der Verfassungsmäßigkeit der Maßnahmen werden auch die Grundsätze relevant sein, die das BVerfG jüngst in der Entscheidung über die Verfassungsbeschwerde hinsichtlich der Vorschriften des Bundeskriminalamtgesetzes (BKAG) zur Terrorismusabwehr aufgestellt hat. Mit einer der für verfassungswidrig erklärten Regelungen, § 20k Abs. 7 S. 3 BKAG, setzt sich der Beitrag auseinander.

Kernbereichsschutz bei heimlichen Überwachungsmaßnahmen

Das BVerfG führt mit dem Urteil vom 20.04.2016 seine Rechtsprechung der vergangenen Jahre im Bereich der staatlichen Überwachungsmaßnahmen fort und überträgt die dort entwickelten Grundsätze auf die Rechtsgrundlagen in §§ 20a ff. BKAG. Es leitet dabei aus dem Verhältnismäßigkeitsgrundsatz vielfältige Anforderungen für die Ausgestaltung dieser Befugnisse ab, wobei dem Schutz des Kernbereichs privater Lebensgestaltung zentrale Bedeutung zukommt. Dieser ergibt sich aus den jeweils betroffenen Grundrechten i. V.m. Art. 1 Abs. 1 GG und sichert dem Einzelnen einen Bereich höchstpersönlicher Privatheit, der nicht überwacht werden darf. Nach der Rechtsprechung des BVerfG ist dem Kernbereichsschutz sowohl bei der Datenerhebung als auch der Datenverwertung

Rechnung zu tragen. Es muss daher möglichst bereits im Vorfeld verhindert werden, dass kernbereichsrelevante Daten überhaupt erhoben werden. Falls solche dennoch erfasst wurden, sind sie in der Regel vor der Verwertung durch die Sicherheitsbehörden von einer unabhängigen Stelle herauszufiltern.

Externe Kontrolle vs. rasche Entscheidung?

Bei einem verdeckten Eingriff in informationstechnische Systeme erhobene Daten sind nach § 20k Abs. 7 S. 3 BKAG unter der Sachleitung des anordnenden Gerichts vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen.

Das BVerfG kommt zu dem Ergebnis, dass § 20k Abs. 7 S. 3 BKAG mit der Verfassung unvereinbar sei, da die Vorschrift keine hinreichend unabhängige Kontrolle der erhobenen Daten vorsehe. Diese setze voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen werde. Dafür müsse die tatsächliche Durchführung und Entscheidungsverantwortung maßgeblich in den Händen von dem Bundeskriminalamt gegenüber unabhängigen Personen liegen. Indem die Sichtung der Daten hier im Wesentlichen Bediensteten des Bundeskriminalamtes selbst obliege, sichere die Vorschrift diesen Standard nicht ab. Daran ändere es auch nichts, dass einer der Bediensteten als behördeninterner Datenschutzbeauftragter nach § 20k Abs. 7 S. 4 BKAG i.V.m. § 4f Abs. 3 BDSG weisungsfrei sei und dass die Sichtung einer allgemein bleibenden „Sachleitung“ des anordnenden Gerichts unterstellt werde.

Das BVerfG verlangt insofern für die Sichtung der Daten aus verdeckten Eingriffen in informationstechnische Systeme, wie auch bei Daten aus Wohnraumüberwachungen, die Einrichtung einer „unabhängigen Stelle“, die die erhobenen Daten auf Kernbereichsrelevanz überprüft und ggf. aussortiert. Eine Verschärfung im Vergleich zur früheren Rechtsprechung ist darin nicht zu sehen, da das BVerfG spätestens seit der Entscheidung zum Großen Lauschangriff stets eine Kontrolle der Verwertbarkeit gewonnener Informationen durch eine „unabhängige Stelle“ gefordert hatte.

Diesem Ergebnis widerspricht das Sondervotum des Richters Schluckebier ausdrücklich: Die Einführung einer „unabhängigen Stelle“, wie sie das BVerfG fordere, werde dem gesetzgeberischen Ziel einer wirksamen Verhinderung terroristischer Straftaten nicht gerecht. Angesichts der häufig bestehenden Eilbedürftigkeit der Datenauswertung müsse die unabhängige Stelle während der Dauer der Überwachungsmaßnahme permanent aktionsfähig sein. Da es sich um eine Maßnahme der Gefahrenabwehr handele, bei der Erhebung und Verwertung der Daten in rascher zeitlicher Folge erfolgten, sei regelmäßig eine schnelle oder sogar sofortige Reaktion auf gewonnene Erkenntnisse erforderlich. Die bestehenden Regelungen seien ausreichend, um den Kernbereichsschutz sicherzustellen.

Wie unabhängig ist unabhängig genug?

Angesichts der divergierenden Ansichten des Senats und des Sondervotums wird deutlich, dass keineswegs Einigkeit darüber besteht, wie die Kontrolle erhobener Daten erfolgen muss. Im Gegensatz zur Wohnraumüberwachung handelt es sich bei einem Zugriff auf informationstechnische Systeme in der Regel um eine einmalige Maßnahme und nicht um eine Dauerüberwachungsaufgabe. Diese erfordert daher lediglich, dass sich die zuständige Person in Bereitschaft befindet und dann ad hoc für die Sichtung der ausgelesenen Daten zur Verfügung steht. Wie Schluckebier zutreffend feststellt, müsste die Person in jedem Fall permanent aktionsfähig sein. Dabei spielt es aber keine Rolle, ob es sich um einen Bediensteten des Bundeskriminalamtes oder um eine „neutrale Stelle“ handelt. Der Einwand Schluckebiers, gerade dies spreche gegen die Einführung einer „unabhängigen Stelle“, überzeugt daher nicht.

Gewährleistung der Vertraulichkeit sensibler Daten

In der Argumentation des BVerfG spiegelt sich die Befürchtung wider, die Vertraulichkeit der gewonnenen kernbereichsrelevanten Informationen könne nicht gewahrt werden. In der Tat besteht die Gefahr, dass durch die starke Einbeziehung der Bediensteten des Bundeskriminalamtes in die Sichtung der Daten Kenntnisse über kernbereichsrelevante Informationen auch in die Hände der mit der konkreten Ermittlung betrauten Personen gelangen. Dies setzt nicht in jedem Fall eine rechtsmissbräuchliche Absicht voraus – bereits ein beiläufiger Austausch unter Kollegen kann die Geheimhaltung sensibler Daten gefährden. Da die kernbereichsrelevanten Daten unter keinen Umständen Einfluss auf die weitere Ermittlung haben dürfen, sind hier wirksame Vorkehrungen zu treffen, um die Vertraulichkeit der Daten sicherzustellen. Aus der Finanzwelt bekannt ist die Errichtung sogenannter „chinese walls“, um den Austausch von Informationen zwischen zwei mit gegenteiligen Zielsetzungen arbeitenden Unternehmensteilen auszuschließen. Die Wirksamkeit solcher Maßnahmen ist freilich umstritten, dem deutschen Recht sind sie aber nicht völlig fremd. So sieht § 6a Abs. 1 EnWG die informatorische Entflechtung vertikal integrierter Energieunternehmen vor, die diese verpflichtet, die Vertraulichkeit wirtschaftlich sensibler Informationen, von denen sie in Ausübung einer Tätigkeit Kenntnis erlangen, gegenüber den anderen Arbeitsbereichen im Unternehmen zu wahren. Die von der Bundesnetzagentur zur Umsetzung dieser Vorschrift herausgegebene Richtlinie ließe sich in Teilen auch für eine wirksame informatorische Trennung zwischen den mit der Sichtung und den mit der Verwertung der Daten betrauten Bediensteten des Bundeskriminalamtes fruchtbar machen.

Das „sachleitende“ Gericht

Unklar ist, welchen Stellenwert die „Sachleitung des Gerichts“ in § 20k Abs. 7 S. 3 BKAG hat und wem in dieser Konstellation die Letztentscheidungsbefugnis über die Kernbereichsrelevanz erhobener Daten zukommt. Was weder in der Argumentation des Senats noch in den beiden abweichenden Meinungen zum Tragen kommt, ist die Entstehungsgeschichte der Vorschrift. Die ursprüngliche Beschlussempfehlung

des Innenausschusses des Bundestages enthielt folgende Formulierung des § 20k Abs. 7 BKAG:

„Erhobene Daten sind unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. […] [6]Besteht zwischen den Beteiligten Uneinigkeit, ob Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, oder hat einer der Beteiligten Zweifel darüber, sind die Daten […] unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit […] vorzulegen."

In der nach Einschaltung des Vermittlungsausschuss beschlossenen Fassung des § 20k Abs. 7 S. 3 BKAG wurde eine stärkere richterliche Einbindung gesehen, mit der der von der Opposition vorgetragenen Forderung nach verstärkter richterlicher Kontrolle über die Sichtung der Daten Rechnung getragen werde. Dennoch ist weder dem Wortlaut der Norm noch den Gesetzgebungsmaterialien zu entnehmen, wie eng die richterliche Kontrolle hier tatsächlich ausfallen muss. Die Bandbreite möglicher Interpretationen der Vorschrift reicht in ihren Extremen von einer bloß beratenden Tätigkeit bis zur ausschließlichen Entscheidungskompetenz des Richters. Es mangelt der Vorschrift daher an Klarheit, die gerade in diesem grundrechtssensiblen Bereich wünschenswert und dringend geboten wäre. Hier muss der Gesetzgeber bei der nun notwendig gewordenen Neuregelung nachbessern. Dabei wäre es auch möglich, die Einbindung des Bundeskriminalamtes in die Sichtung der Daten weiter zu beschränken, indem anstelle des behördeninternen Datenschutzbeauftragen der Bundesdatenschutzbeauftragte damit betraut wird, wie dies in der parlamentarischen Debatte zuweilen gefordert worden war.

Der Gesetzgeber ist wieder am Ball

Es bleibt abzuwarten, in welcher Form der Gesetzgeber den Anforderungen des BVerfG für die Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus gerecht werden wird. Die meisten der beanstandeten Vorschriften, so auch § 20k Abs. 7 S. 3 BKAG, wurden lediglich für mit der Verfassung unvereinbar erklärt und gelten bis maximal zum 30.06.2018 unverändert fort.
